Red Hat Insights 2021

Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities

Last Updated: 2021-09-13

Red Hat Insights 2021 Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities

Legal Notice

Abstract

Generate vulnerability service reports to communicate the exposure of RHEL systems to CVE security vulnerabilities.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

PROVIDING FEEDBACK ON RED HAT HYBRID CLOUD CONSOLE DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so, create a Bugzilla ticket:

1. Go to the Bugzilla website.
2. As the Component, use **Documentation**.
3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
4. Click **Submit Bug**.

CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL VULNERABILITY SERVICE REPORTING

The ability to convey the security exposure of your infrastructure to different stakeholders—DevOps team, security team, executive team—is vital. The vulnerability service enables you to download the following reports to analyze offline or share with others:

- **Executive Reports.** PDF summary and overview of the security vulnerability exposure your infrastructure, intended for executive audiences
- **CVE reports.** PDF report of selected, filtered CVEs to which your infrastructure is exposed, intended to highlight and share vulnerability data
- **Vulnerability data export.** Export of selected CVE data, based on filters you have in place when you perform the export, to a JSON or CSV file

CHAPTER 2. EXECUTIVE REPORTS

You can download a high-level executive report summarizing the security exposure of your infrastructure. Executive reports are two to three-page PDF files, designed for an executive audience, and include the following information:

On page 1

- Number of RHEL systems analyzed
- Number of individual CVEs to which your systems are currently exposed
- Number of security rules in your infrastructure

On page 2

- Percentage of CVEs by severity (CVSS base score) range
- Number of CVEs published by 7, 30, and 90 day time frame
- Top three CVEs in your infrastructure, including security rules and known exploits

On page 3

- Security rule breakdown by severity
- Top 3 security rules, including severity and number of exposed systems

2.1. DOWNLOADING AN EXECUTIVE REPORT

Use the following steps to download an executive report:

Procedure

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > Reports tab and log in if necessary.
2. On the **Executive report** card, click **Download PDF**.
3. Click **Save File** and click **OK**.

Verification

1. Verify that the PDF file is in your **Downloads** folder or other specified location.

2.2. DOWNLOADING AN EXECUTIVE REPORT USING THE VULNERABILITY SERVICE API

You can download an executive report using the vulnerability service API.

- Request URL: https://cloud.redhat.com/api/vulnerability/v1/v1/report/executive
- Curl:

```
curl -X GET "https://cloud.redhat.com/api/vulnerability/v1/v1/report/executive" -H  "accept:
application/vnd.api+json"
```

CHAPTER 3. REPORTS BY CVES

You can create a PDF report showing CVEs to which your systems are exposed. Select CVEs, filtered by severity or security rules, for example, and present curated, focused data to specific stakeholders.

The CVE report lists the CVEs, linking each to the respective CVE page in the Red Hat CVE database so you can learn more about it. The list is ordered primarily by the publish date of the CVE, with the most recently published CVEs at the top of the list.

3.1. EXPORTING A CVE REPORT TO PDF

Use the following procedure to create a point-in-time snapshot of CVEs to which your systems are exposed.

Procedure

1. Navigate to Red Hat Enterprise Linux > Vulnerability > Reports in the Insights for Red Hat Enterprise Linux application. Log in if necessary.
2. On the **Report by CVEs** card, click **Create report**.
3. Make selections as needed in the pop-up card:
    a. Optionally, customize the report title based on the CVEs you are showing.
    b. Under **Filter CVEs by**, click each filter dropdown and select a value.
    c. Under CVE data to include, **Choose columns** is activated by default, allowing you to deselect columns you do not want to include. Leave all boxes checked, or click **All columns** to show everything.
    d. Optionally add notes to give the report context for the audience.
4. Click **Export report** and allow the application a minute to generate the report.
5. Select whether to open or save the PDF file and click **OK**.

Verification

1. Navigate to the saved PDF location and view the CVEs report.

CHAPTER 4. EXPORTING VULNERABILITY DATA AS JSON, CSV, OR PDF FILE

The vulnerability service enables you to export data for CVEs on systems in your RHEL infrastructure. After applying filters in the vulnerability service to view a specific set of CVEs or systems, you can export data based on those criteria.

These reports are accessible through the Insights for Red Hat Enterprise Linux application and can be exported and downloaded as .csv, .json, or PDF files.

4.1. EXPORTING CVE DATA FROM THE VULNERABILITY SERVICE

Perform the following steps to export select data from the vulnerability service.

Procedure

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > CVEs page and log in if necessary.
2. Apply filters and use the sorting functionality at the top of each column to locate specific CVEs.
3. Above the list of CVEs and to the right of the Filters menu, click the **Export** icon,  , and select **Export to JSON**, **Export to CSV**, or **Export as PDF** based on your download preferences.
4. Select a download location and click **Save**.

CHAPTER 5. REFERENCE MATERIALS

To learn more about the vulnerability service, or other Insights for Red Hat Enterprise Linux services and capabilities, the following resources might also be of interest:

- *Assessing and Monitoring Vulnerabilities on RHEL Systems*
- *Remediating Security Exposures using Vulnerability and Ansible Playbooks*
- Insights for Red Hat Enterprise Linux Documentation
- Insights for Red Hat Enterprise Linux Product Support page